Finite Fields and Their Applications 18 (2012) 70–92

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A triple-error-correcting cyclic code from the Gold and Kasami–Welch APN power functions ☆

Xiangyong Zeng [a,*], Jinyong Shan [a], Lei Hu [b]

[a] Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China
[b] The State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing 100049, China

ARTICLE INFO

Article history:
Received 9 April 2010
Revised 23 April 2011
Accepted 22 June 2011
Available online 8 July 2011
Communicated by Gary McGuire

MSC:
94B15
94A60

Keywords:
Cyclic code
BCH code
Triple-error-correcting code
Minimum distance
Almost perfect nonlinear function

ABSTRACT

Based on a sufficient condition proposed by Hollmann and Xiang for constructing triple-error-correcting codes, the minimum distance of a binary cyclic code $\mathcal{C}_{1,3,13}$ with three zeros α, α^3, and α^{13} of length 2^m-1 and the weight divisibility of its dual code are studied, where $m \geqslant 5$ is odd and α is a primitive element of the finite field $\mathbb{F}_{2^m}$. The code $\mathcal{C}_{1,3,13}$ is proven to have the same weight distribution as the binary triple-error-correcting primitive BCH code $\mathcal{C}_{1,3,5}$ of the same length.

1. Introduction

In coding theory, binary triple-error-correcting primitive BCH codes of length $n = 2^m - 1$ are one of the most studied objects [6,15]. Let α be a primitive element of the finite field $\mathbb{F}_{2^m}$ with 2^m elements, and for a subset I of $\mathbb{Z}_{2^m-1}$, let $\mathcal{C}_I$ denote the length-n cyclic code with zeros α^i $(i \in I)$. The primitive BCH code $\mathcal{C}_{1,3,5}$ has minimum distance 7, and its weight distribution was discussed in [19,1–3]. For

☆ The work of X. Zeng and J. Shan was partially supported by the National Natural Science Foundation of China (NSFC) under Grant 60973130. The work of L. Hu was supported by the NSFC (61070172 and 10990011) and the National Basic Research Program of China (2007CB311201).

* Corresponding author.
E-mail addresses: xiangyongzeng@yahoo.com.cn (X. Zeng), shan20051@126.com (J. Shan), hu@is.ac.cn (L. Hu).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2011.06.005

Table 1
Known exponent pairs $\{d_1, d_2\}$ for odd m such that $\mathcal{C}_{1,d_1,d_2}$ and $\mathcal{C}_{1,3,5}$ have the same weight distributions.

$\{d_1, d_2\}$	Condition	
$\{2^r+1, 2^{2r}+1\}$	m odd, $\gcd(m,r)=1$	[20]
$\{2^r+1, 2^{3r}+1\}$	m odd, $\gcd(m,r)=1$	[20]
$\{2^{\frac{m-1}{2}}+1, 2^{\frac{m-1}{2}-1}+1\}$	m odd	[23]
$\{2^{\frac{m+1}{2}}+1, (2^{\frac{m+1}{2}}+1)^2\}$	m odd	[10]

Table 2
Known values of APN power exponents for odd m.

Type	d	Condition	
Gold	2^r+1	$\gcd(r,m)=1$	[14]
Kasami–Welch	$2^{2r}-2^r+1$	$\gcd(r,m)=1$	[20]
Welch	$2^{\frac{m-1}{2}}+3$	m odd	[25]
Niho	$2^{2r}+2^r-1$	$4r\equiv -1 \pmod m$, m odd	[25]
Inverse	$2^{m-1}-1$	m odd	[4,26]
Dobbertin	$2^{4r}+2^{3r}+2^{2r}+2^r-1$	$m=5r$, m odd	[13]

some other integers d_1 and d_2 (they are naturally assumed to be different in the sense of cyclotomic equivalence modulo 2^m-1 and be different to 1), the code $\mathcal{C}_{1,d_1,d_2}$ can also have the same weight distribution as the binary triple-error-correcting primitive BCH code $\mathcal{C}_{1,3,5}$. For example, Table 1 lists all known such exponent pairs $\{d_1, d_2\}$ for odd m, where there exists only one class of exponents with binary weight greater than 2, namely $(2^{\frac{m+1}{2}}+1)^2$ in the construction of [10].

Recently, Hollmann and Xiang [16] proposed a sufficient condition for constructing binary triple-error-correcting codes of length $n=2^m-1$ for odd m. More precisely, for odd m, if a binary cyclic code $\mathcal{C}$ of length $n=2^m-1$ and dimension $n-3m$ has minimum distance at least 7, and if the weights of all codewords of its dual code $\mathcal{C}^\perp$ are divisible by $2^{\frac{m-1}{2}}$, then $\mathcal{C}$ has the same weight distribution as the code $\mathcal{C}_{1,3,5}$. For two exponents d_1 and d_2 such that both x^{d_1} and x^{d_2} are almost perfect nonlinear (APN) power functions from $\mathbb{F}_{2^m}$ to itself, each of the codes $\mathcal{C}_{1,d_1}$ and $\mathcal{C}_{1,d_2}$ has minimum distance exactly 5 by Theorem 5 of [9] (see also Lemma 1 in Section 2). Notice that $\mathcal{C}_{1,d_1,d_2}$ is a subcode of both $\mathcal{C}_{1,d_1}$ and $\mathcal{C}_{1,d_2}$, then $\mathcal{C}_{1,d_1,d_2}$ has minimum distance at least 5. This motivates us to look for suitable APN power exponents d_1 and d_2 such that $\mathcal{C}_{1,d_1,d_2}$ has the same weight distribution as $\mathcal{C}_{1,3,5}$.

Following this idea, we experimentally test all known values of APN power exponents (listed in Table 2) for odd integers $m=5$, 7, 9 and 11, to try to find pairs (d_1, d_2) such that $\mathcal{C}_{1,d_1,d_2}$ and $\mathcal{C}_{1,3,5}$ have the same weight distributions. By the MacWilliams identity for binary linear codes [23], this is equivalent to say that their dual codes $\mathcal{C}^\perp_{1,d_1,d_2}$ and $\mathcal{C}^\perp_{1,3,5}$ have the same weight distributions. The weight distribution of $\mathcal{C}^\perp_{1,3,5}$ is given in [19,23]. The dual code $\mathcal{C}^\perp_{1,d_1,d_2}$ is simply given by

$$\mathcal{C}^\perp_{1,d_1,d_2} = \left\{ \mathbf{c}(\epsilon,\gamma,\delta) = \left(\mathrm{Tr}_1^m\left(\epsilon x + \gamma x^{d_1} + \delta x^{d_2}\right)\right)_{x\in\mathbb{F}_{2^m}^*} \;\middle|\; \epsilon,\gamma,\delta \in \mathbb{F}_{2^m} \right\} \tag{1}$$

and its weight distribution is better to compute than that of the target code $\mathcal{C}_{1,d_1,d_2}$.

All APN exponent pairs (d_1, d_2) such that $\mathcal{C}^\perp_{1,d_1,d_2}$ and $\mathcal{C}^\perp_{1,3,5}$ have the same weight distributions in our experiment are listed in Table 3. For odd m and $\gcd(r,m)=1$, the code $\mathcal{C}_{2^r+1,2^{3r}+1,2^{5r}+1}$ also has the same weight distribution as $\mathcal{C}_{1,3,5}$ [20]. This construction and those in Table 1 can explain all pairs $\{d_1, d_2\}$ without the mark ★ in Table 3. Notice that we say a pair (d_1, d_2) has actually been explained if $\mathcal{C}_{d,2^{i_1}d_1d,2^{i_2}d_2d}$ is proven to have the same weight distribution as $\mathcal{C}_{1,3,5}$ for three integers i_1, i_2, d with $0\leqslant i_1, i_2 \leqslant m-1$, $\gcd(d, 2^m-1)=1$ since $\mathcal{C}_{1,d_1,d_2}$ and $\mathcal{C}_{d,2^{i_1}d_1d,2^{i_2}d_2d}$ have the same weight distributions, where the subscripts are taken modulo 2^m-1.

Table 3
Exponent pairs (d_1, d_2) such that $\mathcal{C}_{1,d_1,d_2}$ and $\mathcal{C}_{1,3,5}$ have the same weight distributions for $m = 5$, 7, 9 and 11.

Exponent pair (d_1, d_2)	$m = 5$	$m = 7$	$m = 9$	$m = 11$
(Gold, Gold)	(3, 5)	(3, 5) (3, 9) (5, 9)	(3, 5) (3, 17) (5, 17)	(3, 5), (3, 9) (3, 17), (3, 33) (5, 9), (5, 17) (5, 33), (9, 17) (9, 33), (17, 33)
(Gold, Kasami–Welch)	(3, 13)	(3, 13)★ (9, 13)	(3, 13)★	(3, 13)★
(Gold, Welch)	(5, 7)	(3, 11) (5, 11)★		
(Gold, Niho)	(3, 5)			
(Kasami–Welch, Welch)	(13, 7)			
(Kasami–Welch, Niho)		(13, 39)		

Indeed, we find a new pair marked by ★ which cannot be explained by known results, where we regard (5, 11) and (3, 13) as a same pair since $\mathcal{C}_{1,5,11}$ has the same weight distribution as $\mathcal{C}_{13,2\times5\times13,2^3\times11\times13}$, i.e., $\mathcal{C}_{1,3,13}$. The new pair consists of the Gold exponent $d_1 = 3$ and Kasami–Welch exponent $d_2 = 13$, and d_2 is another example of exponents with binary weight 3.

This paper will prove that for any odd integer $m \geqslant 5$, the code $\mathcal{C}_{1,3,13}$ has the same weight distribution as $\mathcal{C}_{1,3,5}$. To this end, we use a method developed by Hollmann and Xiang in [16,17] which analyzes the divisibility of the weights of the codewords in $\mathcal{C}^{\perp}_{1,3,13}$ by an add-with-carry algorithm and a technical graph-theoretic deduction. In Ref. [16], Hollmann and Xiang also applied this method to study the code $\mathcal{C}_{1,d_1,d_2}$ proposed in [10], where $d_1 = 2^{\frac{m+1}{2}} + 1$ and $d_2 = (2^{\frac{m+1}{2}} + 1)^2$. Recently, Leander and Langevin in [21] applied the method of Hollmann and Xiang to study the code $\mathcal{C}_{1,13/3}$ and the weight divisibility of the codewords in this code.

The remainder of this paper is organized as follows. Section 2 gives some preliminaries and the results of this paper. Section 3 establishes a lower bound on the minimum distance of the code $\mathcal{C}_{1,3,13}$. Section 4 discusses the weight divisibility of $\mathcal{C}^{\perp}_{1,3,13}$. Section 5 concludes the study.

2. Preliminaries and the results

Let $\mathbb{F}^*_{2^m} = \mathbb{F}_{2^m} \setminus \{0\}$. The trace function Tr_1^m from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ is defined by [22, p. 54]

$$\mathrm{Tr}_1^m(x) = \sum_{i=0}^{m-1} x^{2^i}, \quad x \in \mathbb{F}_{2^m}.$$

A binary cyclic code $\mathcal{C}$ of length n is a principal ideal in the ring $\mathbb{F}_2[x]/(x^n - 1)$. If $g(x)$ is a generator polynomial of $\mathcal{C}$, then a power β of a primitive n-th root of unity is a zero of the code $\mathcal{C}$ if and only if $g(\beta) = 0$. A codeword c in $\mathcal{C}$ has the form as $c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$, which corresponds to a binary vector $(c_0, c_1, \ldots, c_{n-1})$. The Hamming weight of the codeword c is the number of nonzero c_i for $0 \leqslant i \leqslant n-1$, denoted by $wt(c)$.

Definition 1. A function f from $\mathbb{F}_{2^m}$ to itself is said to be almost perfect nonlinear (APN) if for each $e \in \mathbb{F}^*_{2^m}$, the function $\Delta_{f,e}(x) = f(x + e) + f(x)$ is two-to-one from $\mathbb{F}_{2^m}$ to itself.

APN functions were introduced in [26] by Nyberg to define them as the mappings with highest resistance to differential cryptanalysis. For more details we refer the reader to [4,7,8,11–14,18,20,26] and the references therein.

For a function f from $\mathbb{F}_{2^m}$ to itself with $f(0)=0$, let $\mathcal{C}_f$ denote the binary cyclic code of length $n=2^m-1$ with parity check matrix

$$H_f=\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{2^m-2}) \end{pmatrix}$$

where α is a primitive element of $\mathbb{F}_{2^m}$, and each entry is viewed as a binary column vector basing on a basis expression of elements of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$.

The APN properties of f can be characterized by the minimum distance of $\mathcal{C}_f$ [9].

Lemma 1. *(See [9].) The code $\mathcal{C}_f$ has minimum distance 5 if and only if f is APN.*

Since the 1960s, the family of triple-error-correcting binary primitive BCH codes of length $n=2^m-1$ has been thoroughly studied. The following lemma given by Hollmann and Xiang presented a sufficient condition for constructing families of triple-error-correcting codes.

Lemma 2. *(See [16].) Let m be odd and $\mathcal{C}$ be a binary cyclic code of length $n=2^m-1$, dimension $n-3m$ and minimum distance at least 7. If all weights of the codewords in $\mathcal{C}^\perp$ are divisible by $2^{\frac{m-1}{2}}$, then $\mathcal{C}$ has the same weight distribution as $\mathcal{C}_{1,3,5}$.*

With Lemma 2, for odd m, we can construct binary triple-error-correcting codes of length $n=2^m-1$ and dimension $n-3m$ by analyzing their minimum distances and weight divisibility of their dual codes. The following Proposition 1 will be proven in the next section, and the following Lemma 3 shows that the product of the nonzeros of a binary cyclic code can be used to analyze the weight divisibility.

Proposition 1. *For odd $m\geqslant 5$, the code $\mathcal{C}_{1,3,13}$ has minimum distance at least 7.*

Lemma 3 *(McEliece's Theorem). (See [24].) Let $\mathcal{C}$ be a binary cyclic code, and let l be the smallest positive integer such that l nonzeros of $\mathcal{C}$ (with repetitions allowed) have product 1. Then the weight of every codeword in $\mathcal{C}$ is divisible by 2^{l-1}, and there is at least one codeword whose weight is not divisible by 2^l.*

The following definition can be used to obtain information on the largest power of 2 dividing the weights of all codewords of a binary cyclic code as below [16,17].

Definition 2. For a positive integer m and a non-negative integer a with the binary expression $a=\sum_{i=0}^{m-1}a_i2^i$, $a_i\in\{0,1\}$, the (binary) weight $w(a)$ of a is defined as the integer $w(a)=\sum_{i=0}^{m-1}a_i$. For $d_1,d_2,\ldots,d_h\in\mathbb{Z}_{2^m-1}$, define

$$M(m;d_1,d_2,\ldots,d_h)=\max\left(w(s)-\sum_{l=1}^{h}w\big(a^{(l)}\big)\right)$$

where the maximum is taken over all integers $s,a^{(1)},\ldots,a^{(h)}$ satisfying

$$0\leqslant s,a^{(1)},\ldots,a^{(h)}\leqslant 2^m-1,\qquad s\equiv\sum_{l=1}^{h}d_la^{(l)}\pmod{2^m-1}$$

and

$$a^{(l)}\not\equiv 0\pmod{2^m-1}\quad\text{for some } l.$$

The add-with-carry algorithm for integers modulo $2^m - 1$ can be used to determine $M(m; d_1, d_2, \ldots, d_h)$ [16,17], and it will be recalled in Section 4.1.

Lemma 4. *(See [16,17].) All the weights of the codewords in $\mathcal{C}^{\perp}_{1,d_1,d_2}$ are divisible by $2^{m-M(m;d_1,d_2)-1}$, and there is at least one codeword whose weight is not divisible by $2^{m-M(m;d_1,d_2)}$.*

The following proposition will be proven in Section 4.

Proposition 2. $M(m; 3, 13) = (m-1)/2$.

By Propositions 1 and 2 and Lemmas 2 and 4, we obtain the following theorem as the main result in this paper.

Theorem 1. *For any odd integer $m \geqslant 5$, the code $\mathcal{C}_{1,3,13}$ has the same weight distribution as the binary triple-error-correcting primitive BCH code $\mathcal{C}_{1,3,5}$.*

3. Minimum distance of $\mathcal{C}_{1,3,13}$

In the paper [27], Schaub showed that the minimum distance of a linear cyclic code is equal to the rank of a matrix constructed by using Discrete Fourier Transform. This together with BCH or HT bound established a lower bound on the minimum distance of the code proposed in [10]. In the proof of Proposition 1, we apply this method and the results for the minimum distances of the cyclic codes $\mathcal{C}_{1,3,5}$ and $\mathcal{C}_{1,3,9}$ [20] to obtain a lower bound on minimum distance of $\mathcal{C}_{1,3,13}$.

Proof of Proposition 1. Let $c = (c_0, c_1, \ldots, c_{n-1})$ be an arbitrary codeword in $\mathcal{C}_{1,3,13}$, where $n = 2^m - 1$. Let α be a primitive element of $\mathbb{F}_{2^m}$, and the Discrete Fourier Transform of c is the sequence $\{A_\lambda\}$ with

$$A_\lambda = \sum_{i=0}^{n-1} c_i \alpha^{i\lambda}, \quad 0 \leqslant \lambda < n.$$

From the above formula, we have that n is a period of the sequence $\{A_\lambda\}$. If $A_5 = 0$, then c is a codeword of the code $\mathcal{C}_{1,3,5}$ which has minimum distance 7 [20]. This shows $wt(c) \geqslant 7$. If $A_9 = 0$, then c is a codeword of the code $\mathcal{C}_{1,3,9}$ which also has minimum distance 7 [20]. Consequently, $wt(c) \geqslant 7$. Thus we can assume that $A_5 A_9 \neq 0$ in the following analysis.

By [27], the Hamming weight of c equals to the linear complexity (also called linear span) of the sequence $\{A_\lambda\}$. It is sufficient to prove that the rank of M is at least 7, where

$$M = \begin{pmatrix} A_0 & A_1 & \cdots & A_{n-1} \\ A_1 & A_2 & \cdots & A_0 \\ \vdots & \vdots & & \vdots \\ A_{n-1} & A_0 & \cdots & A_{n-2} \end{pmatrix}. \tag{2}$$

To this end, we will argue separately according to the parity of $wt(c)$.

(1) Suppose that $wt(c)$ is odd, i.e., $A_0 = 1$.

In this case, we will find two submatrices M_1 and M_2 of M such that either M_1 or M_2 has full rank, where

$$M_1 = \begin{pmatrix} A_0 & A_1 & A_2 & A_4 & A_6 & A_8 \\ A_1 & A_2 & A_3 & A_5 & A_7 & A_9 \\ A_2 & A_3 & A_4 & A_6 & A_8 & A_{10} \\ A_3 & A_4 & A_5 & A_7 & A_9 & A_{11} \\ A_5 & A_6 & A_7 & A_9 & A_{11} & A_{13} \\ A_6 & A_7 & A_8 & A_{10} & A_{12} & A_{14} \end{pmatrix}$$

and

$$M_2 = \begin{pmatrix} A_0 & A_1 & A_3 & A_4 & A_7 & A_8 \\ A_1 & A_2 & A_4 & A_5 & A_8 & A_9 \\ A_2 & A_3 & A_5 & A_6 & A_9 & A_{10} \\ A_3 & A_4 & A_6 & A_7 & A_{10} & A_{11} \\ A_4 & A_5 & A_7 & A_8 & A_{11} & A_{12} \\ A_5 & A_6 & A_8 & A_9 & A_{12} & A_{13} \end{pmatrix}.$$

Notice that $A_\lambda = 0$ if $\lambda \in C_1 \cup C_3 \cup C_{13}$, where C_i denotes the cyclotomic coset modulo $2^m - 1$ containing the integer i. Consequently, we have

$$A_1 = A_2 = A_3 = A_4 = A_6 = A_8 = A_{12} = A_{13} = 0.$$

From the expression of A_λ, we have $A_{10} = A_5^2$, $A_{14} = A_7^2$ and $A_{18} = A_9^2$.

It can be directly verified that

$$\det(M_1) = A_5^2 A_7\big(A_7^3 + A_5^2 A_{11}\big) \quad \text{and} \quad \det(M_2) = A_5^2\big(A_5^2 A_9^2 + A_5 A_9 A_7^2 + A_5^2 A_7 A_{11}\big).$$

If $A_7 = 0$, then $\det(M_2) = A_5^4 A_9^2 \neq 0$ by our assumption that $A_5 A_9 \neq 0$, i.e., $\operatorname{rank}(M_2) = 6$. If $A_7 \neq 0$ and $A_{11} = 0$, then $\det(M_1) \neq 0$ by $A_5 A_7 \neq 0$, i.e., M_1 has rank 6. If $A_7 \neq 0$, $A_{11} \neq 0$ and $\det(M_1) = 0$, then $A_7^3 = A_5^2 A_{11}$. Thus,

$$\det(M_2) = A_5^2\big(A_5^2 A_9^2 + A_5 A_9 A_7^2 + A_7^4\big), \tag{3}$$

which is either $A_5^3 A_9 A_7^2 \neq 0$ if $A_5 A_9 = A_7^2$ or $A_5^2(A_5 A_9 + A_7^2)^{-1}[(A_5 A_9)^3 + (A_7^2)^3] \neq 0$ since $\gcd(3, n) = 1$ if $A_5 A_9 \neq A_7^2$. Therefore, either M_1 or M_2 has full rank, and then $\operatorname{rank}(M) \geqslant 6$. As a consequence, $wt(c) \geqslant 7$.

(2) Suppose that $wt(c)$ is even, i.e., $A_0 = 0$.

If $A_7 = 0$, consider the following submatrix

$$M_3 = \begin{pmatrix} A_0 & A_1 & A_2 & A_4 & A_5 & A_6 & A_8 \\ A_1 & A_2 & A_3 & A_5 & A_6 & A_7 & A_9 \\ A_2 & A_3 & A_4 & A_6 & A_7 & A_8 & A_{10} \\ A_4 & A_5 & A_6 & A_8 & A_9 & A_{10} & A_{12} \\ A_5 & A_6 & A_7 & A_9 & A_{10} & A_{11} & A_{13} \\ A_7 & A_8 & A_9 & A_{11} & A_{12} & A_{13} & A_{15} \\ A_8 & A_9 & A_{10} & A_{12} & A_{13} & A_{14} & A_{16} \end{pmatrix}.$$

By a direct calculation, we have $\det(M_3) = A_5^7 A_9^2 \neq 0$. Thus $\operatorname{rank}(M_3) \geqslant 7$ which implies that $wt(c) \geqslant 7$.

If $A_7 \neq 0$, consider the following submatrix

$$M_4 = \begin{pmatrix} A_0 & A_1 & A_2 & A_4 & A_6 & A_7 & A_8 \\ A_1 & A_2 & A_3 & A_5 & A_7 & A_8 & A_9 \\ A_2 & A_3 & A_4 & A_6 & A_8 & A_9 & A_{10} \\ A_4 & A_5 & A_6 & A_8 & A_{10} & A_{11} & A_{12} \\ A_5 & A_6 & A_7 & A_9 & A_{11} & A_{12} & A_{13} \\ A_8 & A_9 & A_{10} & A_{12} & A_{14} & A_{15} & A_{16} \\ A_{12} & A_{13} & A_{14} & A_{16} & A_{18} & A_{19} & A_{20} \end{pmatrix}.$$

By a direct calculation, we have $\det(M_4) = A_5^5 A_7 (A_5^2 A_9^2 + A_5 A_9 A_7^2 + A_7^4)$. With a similar analysis as for (3), we have $\det(M_4) \neq 0$ and then $\operatorname{rank}(M) \geqslant 7$. Thus, $wt(c) \geqslant 7$. □

4. Divisibility of weights in $\mathcal{C}^{\perp}_{\mathbf{1,3,13}}$

In this section, for an odd integer $m = 2k+1$ with $k \geqslant 2$, we will prove $M(m; 3, 13) = k$.

4.1. Modular add-with-carry algorithms in $\mathbb{Z}_{2^m-1}$

Let $a^{(l)}$ and s have the binary expressions

$$a^{(l)} = \sum_{i=0}^{m-1} a_i^{(l)} 2^i \quad \text{for } 1 \leqslant l \leqslant j \quad \text{and} \quad s = \sum_{i=0}^{m-1} s_i 2^i, \tag{4}$$

respectively. Furthermore, let $\mu_1, \mu_2, \ldots, \mu_j$ be nonzero integers, and define $\mu_+ = \sum_{\mu_l > 0} \mu_l$ and $\mu_- = \sum_{\mu_l < 0} \mu_l$ so that $\sum_{l=1}^{j} \mu_l = \mu_+ + \mu_-$, $\mu_+ \geqslant 0$, $\mu_- \leqslant 0$, and suppose that $s \equiv \mu_1 a^{(1)} + \mu_2 a^{(2)} + \cdots + \mu_j a^{(j)} \pmod{2^m - 1}$.

Lemma 5. *(See [16,17].) There exists a unique integer sequence $c_{-1}, c_0, \ldots, c_{m-1}$ with $c_{-1} = c_{m-1}$ such that*

$$2c_i + s_i = \sum_{l=1}^{j} \mu_l a_i^{(l)} + c_{i-1}, \quad 0 \leqslant i \leqslant m-1 \tag{5}$$

holds. Moreover, with notation $w(c) = \sum_{i=0}^{m-1} c_i$, we have that

$$w(c) = \sum_{l=1}^{j} \mu_l w\big(a^{(l)}\big) - w(s).$$

The numbers c_i satisfy $\mu_- - 1 \leqslant c_i \leqslant \mu_+$, and further

$$\mu_- \leqslant c_i < \mu_+$$

for all i if $a^{(l)} \not\equiv 0 \pmod{2^m - 1}$ holds for some l.

The integers s_i and c_i are called the *digits* and *carries* for the computation of s modulo $2^m - 1$ in terms of $a^{(1)}, \ldots, a^{(j)}, \mu_1, \ldots, \mu_j$.

4.2. Determination of the value $M(m; 3, 13)$

Let s, a and b be integers with $0 \leqslant s, a, b \leqslant 2^m - 1$, $s \equiv 3a + 13b \pmod{2^m - 1}$, and assume that at least one of a and b is nonzero modulo $2^m - 1$. Let $s = \sum_{i=0}^{m-1} s_i 2^i$, $a = \sum_{i=0}^{m-1} a_i 2^i$, and $b = \sum_{i=0}^{m-1} b_i 2^i$ be the binary expressions of s, a and b, respectively.

We first prove $M(m; 3, 13) \leqslant k$, namely $w(s) - w(a) - w(b) \leqslant k$ in the sequel.

Notice that $2a$, $8b$, $4b \pmod{2^m - 1}$ have the binary expressions $\sum_{i=0}^{m-1} a_{i-1} 2^i$, $\sum_{i=0}^{m-1} b_{i-3} 2^i$, $\sum_{i=0}^{m-1} b_{i-2} 2^i$, respectively, and $s \equiv 3a + 13b \equiv 2a + a + 8b + 4b + b \pmod{2^m - 1}$. Taking $\mu_l = 1$ for $l \in \{1, 2, 3, 4, 5\}$ and $a^{(1)} = 2a$, $a^{(2)} = a$, $a^{(3)} = 8b$, $a^{(4)} = 4b$, $a^{(5)} = b$ and applying Lemma 5, there are carries $c_i \in \{0, 1, 2, 3, 4\}$ such that

$$2c_i + s_i = a_{i-1} + a_i + b_{i-3} + b_{i-2} + b_i + c_{i-1}, \quad 0 \leqslant i \leqslant m - 1, \tag{6}$$

where the subscripts are taken modulo m. With $w(c) = \sum_{i=0}^{m-1} c_i$, by the m equalities in (6) we have

$$w(c) + w(s) = 2w(a) + 3w(b). \tag{7}$$

Let

$$\nu_i = a_{i-1} + a_i + b_{i-3} + b_{i-2} + b_{i-1} + b_i - c_{i-1} - c_i, \quad 0 \leqslant i \leqslant m - 1 \tag{8}$$

and $w(\nu) = \sum_{i=0}^{m-1} \nu_i$. Then by (8) and (7), we have

$$w(\nu) = 2w(a) + 4w(b) - 2w(c) = 2\big(w(s) - w(a) - w(b)\big). \tag{9}$$

To prove $w(s) - w(a) - w(b) \leqslant k$, by (9) it is sufficient to prove $w(\nu) \leqslant m$. To this end, we will define a certain weighted directed graph $\mathbb{D}$ and recall some related definitions in [5] as below.

A *directed graph* $\mathbb{D}$ is an ordered pair $(V(\mathbb{D}), A(\mathbb{D}))$ consisting of a set $V(\mathbb{D})$ of vertices and a set $A(\mathbb{D})$, disjoint from $V(\mathbb{D})$, of *arcs*, together with an *incidence function* $\psi_{\mathbb{D}}$ that associates with each arc ϑ of $\mathbb{D}$ an ordered pair of (not necessarily distinct) vertices $\psi_{\mathbb{D}}(\vartheta) = (T(\vartheta), H(\vartheta))$ of $\mathbb{D}$. The vertex $T(\vartheta)$ is the *tail* of ϑ, and the vertex $H(\vartheta)$ its *head*. For each arc ϑ in a directed graph $\mathbb{D}$, we can associate a real number $w(\vartheta)$ with ϑ, and $w(\vartheta)$ is called its *weight*. In this case, $\mathbb{D}$ is called to be a *weighted directed graph*. In a directed graph $\mathbb{D}$, a *directed walk* is an alternating sequence of vertices and arcs

$$W := P_0 \vartheta_0 P_1 \cdots P_{l-1} \vartheta_{l-1} P_l$$

such that for each i with $1 \leqslant i \leqslant l$, P_{i-1} and P_i are the tail and head of ϑ_{i-1}, respectively. In this case, we refer to W as a *directed* (P_0, P_l)*-walk*. For two vertices P_i and P_j in the walk W where $0 \leqslant i < j \leqslant l$, the (P_i, P_j)*-segment* of W is the subsequence of W starting with P_i and ending with P_j, and it is denoted $P_i W P_j$. The directed walk W in $\mathbb{D}$ is *closed* if its initial and terminal vertices P_0, P_l are identical.

With these preparations, we can define a weighted directed graph $\mathbb{D}$. The vertices of $\mathbb{D}$ consist of all vectors $P = (x, y, z, u)$, where $x, y, z \in \{0, 1\}$ and $u \in \{0, 1, 2, 3, 4\}$. Let $P_1 = (x_1, y_1, z_1, u_1)$ and $P_2 = (x_2, y_2, z_2, u_2)$ be two vertices of $\mathbb{D}$, and define an arc ϑ with $T(\vartheta) = P_1$ and $H(\vartheta) = P_2$ if

$$x_1 + y_1 + z_1 + x_2 + z_2 - 2u_1 + u_2 = 0, \text{ or } 1. \tag{10}$$

The weight of the arc ϑ is defined as

$$w(\vartheta) = x_1 + y_1 + z_1 + x_2 + y_2 + z_2 - u_1 - u_2.$$

Table 4
The weight distribution of all arcs in the weighted directed graph $\mathbb{D}$.

Weight	-6	-5	-4	-3	-2	-1	0	1	2	3	4
The number of arcs	1	16	36	43	43	42	43	43	36	16	1

Thus for $i \in \{0, 1, \ldots, m-1\}$,

$$V_i = (a_i, b_i, b_{i-2}, c_i) \tag{11}$$

are m vertices of $\mathbb{D}$, where a_i, b_i, and c_i are those integers in (6). Furthermore, there are m arcs ϑ_i with $w(\vartheta_i) = \nu_i$ defined by (8) with the tail $V_i = (a_i, b_i, b_{i-2}, c_i)$ and head $V_{i-1} = (a_{i-1}, b_{i-1}, b_{i-3}, c_{i-1})$ for all $0 \leqslant i \leqslant m-1$ since $a_i + b_i + b_{i-2} + a_{i-1} + b_{i-3} - 2c_i + c_{i-1} = s_i \in \{0, 1\}$ by (6), where the subscripts are taken modulo m. With the above preparation, we define a set

$$\mathcal{P}_0 = \left\{ W = P_0\vartheta_0 P_1\vartheta_1 \cdots P_{m-1}\vartheta_{m-1}P_m \;\middle|\; P_i = V_{m-i-1},\ a, b \in \mathbb{Z}_{2^m-1} \right\}. \tag{12}$$

Observing the set $\mathcal{P}_0$, we find some properties as (i) any walk $W \in \mathcal{P}_0$ is closed; (ii) $V_i(3) = V_{i-2}(2) = b_{i-2}$ with $0 \leqslant i \leqslant m-1$, where the subscripts are taken modulo m.

With the help of a computer, we have that there are totally 320 arcs in $\mathbb{D}$, and their weight distribution is given in Table 4. Furthermore, any vertex in the set

$$\Gamma = \left\{ (1,1,0,0), (1,0,1,0), (0,1,1,0), (1,1,1,0) \right\} \tag{13}$$

cannot be the tail of any arc in $\mathbb{D}$. Some arcs ϑ with head $H(\vartheta) \notin \Gamma$ will be used in this section and they are listed in Appendix A.

Notice that for the case $\nu_i < 2$ for all $i \in \{0, 1, \ldots, m-1\}$, it can be easily verified that $w(\nu) \leqslant m$. Consequently, the proof for $w(\nu) \leqslant m$ can be proceeded in two steps as below.

Step 1. To prove that for any $\nu_i \geqslant 2$, there exists a positive integer $t_i \leqslant m$ such that $\nu_i + \nu_{i-1} + \cdots + \nu_{i-t_i+1} \leqslant t_i$.

Step 2. Based on Step 1, we will prove $w(\nu) = \sum_{i=0}^{m-1} \nu_i \leqslant m$.

The two steps are summarized as the following Propositions 3 and 4.

Proposition 3. *For any $\nu_i \geqslant 2$, there exists a positive integer $t_i \leqslant m$ such that $\nu_i + \nu_{i-1} + \cdots + \nu_{i-t_i+1} \leqslant t_i$, where the subscripts are taken modulo m.*

By the weighted directed graph $\mathbb{D}$ defined as above, the number $\nu_i + \nu_{i-1} + \cdots + \nu_{i-t_i+1}$ can be regarded as the sum of the weights of some arcs in $\mathbb{D}$ (more precisely, these arcs are in $\mathcal{P}_0$). To finish the proof of Proposition 3, we only need to consider the walk set $\mathcal{P}_0$. Indeed, to prove Proposition 3, we consider a related set $\mathcal{P}$, which is defined as

$$\begin{aligned} \mathcal{P} = \Big\{ & W = P_0\vartheta_0 P_1 \cdots P_{i-1}\vartheta_{i-1}P_i\vartheta_i \cdots P_{q-1}\vartheta_{q-1}P_q \;\Big|\; W \in \mathbb{D} \text{ satisfies} \\ & \text{the properties (I), (II) and (III), and } q \text{ is dependent on } W \Big\} \end{aligned} \tag{14}$$

where the properties (I), (II) and (III) are as below respectively:

(I) any vertex of the set Γ in (13) does not occur in W;
(II) for $0 \leqslant i \leqslant q-2$, any three consecutive vertices P_i, P_{i+1}, and P_{i+2} in W satisfy $P_i(3) = P_{i+2}(2)$, where $P_i(l)$ denotes the l-th component of P_i for $l \in \{1,2,3,4\}$; in addition, if the walk W is closed, then $P_{q-1}(3) = P_1(2)$;
(III) any arc ϑ_i in W satisfies that $w(\vartheta_i) \geqslant (i+2) - T_i$ for $0 \leqslant i \leqslant q-1$, where $T_0 = 0$ and $T_i = \sum_{l=0}^{i-1} w(\vartheta_l)$ for $i \geqslant 1$.

Remark 1. If a vertex $P \in \Gamma$ occurs in some walk W, then W is not closed and it must not be in $\mathcal{P}_0$. Therefore, we will consider the walks satisfying the property (I). If $P_i\vartheta_i P_{i+1}\vartheta_{i+1}P_{i+2}$ occurs in some walk W with $P_i(3) \neq P_{i+2}(2)$, then W must not be in $\mathcal{P}_0$, either. Thus, the property (II) should be considered too. For any sequence $\nu_0, \nu_1, \ldots, \nu_{m-1}$ determined by $a, b \in \mathbb{Z}_{2^m-1}$ in Proposition 3, there exists one walk $W \in \mathcal{P}_0$ with $w(\vartheta_i) = \nu_{m-i-1}$. If a sequence $\nu_0, \nu_1, \ldots, \nu_{m-1}$ does not satisfy Proposition 3, then there exists $\nu_{m-i-1} \geqslant 2$ such that $\nu_{m-i-1} + \cdots + \nu_{m-i-t} \geqslant t+1$ for any positive integer t. Then we have $w(\vartheta_i) + \cdots + w(\vartheta_{i+t-1}) \geqslant t+1$, i.e., $w(\vartheta_{i+t}) \geqslant t+2-\sum_{l=i}^{i+t-1} w(\vartheta_l)$. Thus, we only need to consider the walks in $\mathcal{P}_0$ satisfying the property (III) and these walks are all in the walk set $\mathcal{P}$. Consequently, considering the set $\mathcal{P}$ is enough.

If Proposition 3 is not true, then there is an integer i_0 with $0 \leqslant i_0 \leqslant m-1$ such that $\nu_{i_0} \geqslant 2$ and $\nu_{i_0} + \nu_{i_0-1} + \cdots + \nu_{i_0-t+1} \geqslant t+1$ for any positive integer t with $2 \leqslant t \leqslant m$. Let

$$W_0 = P_0\vartheta_0 P_1\vartheta_1 \cdots P_{i-1}\vartheta_{i-1}P_i\vartheta_i \cdots P_{m-2}\vartheta_{m-2}P_{m-1}\vartheta_{m-1}P_m \tag{15}$$

be the walk such that $P_i = V_{i_0-i}$ in (11) for $0 \leqslant i \leqslant m-1$, and ϑ_i be the arc with $T(\vartheta_i) = P_i$ and $H(\vartheta_i) = P_{i+1}$ for $i \in \{0,1,\ldots,m-1\}$, where the subscripts are taken modulo m. Then, we have $w(\vartheta_0) \geqslant 2$ and for any positive integer t with $2 \leqslant t \leqslant m$ such that $w(\vartheta_0) + w(\vartheta_1) + \cdots + w(\vartheta_{t-1}) \geqslant t+1$. Thus by (11) and the analysis therein, $W_0 \in \mathcal{P}$ and it is closed. As a consequence, it will lead to a contradiction if any walk $W \in \mathcal{P}$ is not closed. In fact, we can prove that any walk $W \in \mathcal{P}$ is not closed in the sequel. This will give the proof of Proposition 3.

The following notations are used throughout this section:

- $P_i \xrightarrow{(\eta,\omega)}$ denotes any walk $P_i\vartheta_i P_{i+1}$ with $T(\vartheta_i) = P_i$, $H(\vartheta_i) = P_{i+1}$, $P_{i+1}(2) = \eta$ and $w(\vartheta_i) \geqslant \omega$;
- $P_i \xrightarrow{(-,\omega)}$ denotes any walk $P_i\vartheta_i P_{i+1}$ with $T(\vartheta_i) = P_i$, $H(\vartheta_i) = P_{i+1}$, $P_{i+1}(2) \in \{0,1\}$ and $w(\vartheta_i) \geqslant \omega$;
- $P_i \xrightarrow{(\eta,\omega)} O$ denotes that there does not exist any arc ϑ such that $T(\vartheta) = P_i$, $H(\vartheta) \in \mathbb{D}$, $(H(\vartheta))(2) = \eta$ and $w(\vartheta) \geqslant \omega$.

With the above notations, we can conveniently describe the walks in $\mathcal{P}$.

Example 1. Let q be a positive integer and $\omega = (j+2) - T_j = 1$ for some positive integer j with $0 \leqslant j < q$, and let

$$W\colon \quad P_0 \to P_1 \to \cdots \to P_{j-1} \to P_j = (0,0,0,0) \xrightarrow{(0,\omega)} P_{j+1} \to \cdots \to P_q$$

be a walk in the set $\mathcal{P}$, and ϑ_i be the arc with the tail P_i and head P_{i+1} for each $i \in \{0,1,\ldots,q-1\}$. By Appendix A, we can find all possibilities for the segment $P_{j+1}WP_q$, which is completely determined by the walk $(0,0,0,0) \xrightarrow{(0,1)}$.

If we find all possibilities for the segment $P_{j+1}WP_q$, then we also know all possibilities for the segment $P_{j+1}WP_{q'}$ for any integer $j+1 \leqslant q' \leqslant q$. Therefore, without loss of generality, we can assume that the integer q is large enough.

Since $P_{j+1}(2) = 0$ and $w(\vartheta_j) \geqslant 1$, by Appendix A, we have $P_{j+1} \in \{(1,0,0,0),(0,0,1,0)\}$. If $P_{j+1} = (1,0,0,0)$, by properties (II) and (III) of the walks in $\mathcal{P}$, we have $P_{j+2}(2) = P_j(3) = 0$ and

$w(\vartheta_{j+1}) \geqslant (j+3) - T_{j+1} = (j+3) - w(\vartheta_j) - T_j = (j+2) - w(\vartheta_j) - T_j = 1$. By Appendix A, we can uniquely determine $P_{j+2} = (0,0,0,0)$. Furthermore, with $w(\vartheta_{j+1}) = 1$ and $P_{j+1} = (1,0,0,0)$, we have

$$w(\vartheta_{j+2}) \geqslant (j+4) - T_{j+2} = (j+4) - w(\vartheta_{j+1}) - T_{j+1} = (j+3) - T_{j+1} = 1 \tag{16}$$

and $P_{j+3}(2) = 0$. Therefore, for $P_{j+1} = (1,0,0,0)$, $P_{j+1}WP_{j+3}$ can be expressed as

$$(1,0,0,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(0,1)} . \tag{17}$$

Similarly, for $P_{j+1} = (0,0,1,0)$, $P_{j+1}WP_{j+5}$ is given by

$$(0,0,1,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(1,1)} (0,1,0,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(0,1)} . \tag{18}$$

Combining (17) and (18), we have an expression consisting of two segments with initial vertex P_j

$$(0,0,0,0) \xrightarrow{(0,1)} \begin{cases} (1,0,0,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(0,1)} \\ (0,0,1,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(1,1)} (0,1,0,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(0,1)} . \end{cases} \tag{19}$$

In the first segment of (19), $P_{j+3} = (1,0,0,0)$ or $(0,0,1,0)$ since the walk $(0,0,0,0) \xrightarrow{(0,1)}$ has only two possible forms, which have occurred as P_jWP_{j+1} in the first and second segments of (19), respectively. By a similar analysis, we have $P_{j+5} = (1,0,0,0)$ or $(0,0,1,0)$ in the second segment of (19). Therefore, again by (19), we have that $P_{j+3}WP_{j+5}$ has the form as (17) or $P_{j+3}WP_{j+7}$ has the form as (18) in the first segment of (19). Similarly, we have that $P_{j+5}WP_{j+7}$ has the form as (17) or $P_{j+5}WP_{j+9}$ has the form as (18) in the second segment of (19). Repeating the above process, all possibilities of $P_{j+1}WP_q$ can be obtained. Further, all vertices P_l $(j \leqslant l \leqslant q)$ have occurred in the two segments of (19), and they are $(0,0,0,0)$, $(1,0,0,0)$, $(0,1,0,0)$, and $(0,0,1,0)$.

Remark 2. In Example 1, $(0,0,0,0) \xrightarrow{(0,1)}$ completely determines all possibilities for the segment $P_{j+1}WP_q$ of W. The expression (19) consists of two basic segments of W, by which all possibilities of the segment $P_{j+1}WP_q$ can be conveniently found. In the proofs of Lemmas 6 and 7, for some given $P_j \xrightarrow{(\eta,\omega)}$ of a walk W in $\mathcal{P}$, we will frequently need to determine all possibilities for the segment $P_{j+1}WP_q$ of W. Similarly as in Example 1, we will use some expression consisting of basic segments of W to determine all possibilities of $P_{j+1}WP_q$. We call the expression as (19) *a set of basic segments* (SBS) of $P_j \xrightarrow{(\eta,\omega)}$.

The following two lemmas will be used to prove Proposition 3.

Lemma 6. *Let q be a positive integer and $\omega = (j+2) - T_j$ for some positive integer j with $0 \leqslant j < q$. For any walk*

$$W\colon \quad P_0 \to P_1 \to \cdots \to P_{j-1} \to P_j = (0,0,0,0) \xrightarrow{(-,\omega)} P_{j+1} \to \cdots \to P_q$$

in the set $\mathcal{P}$ defined by (14)*, we have*

(i) *if $\omega = 0$ or 1, all vertices P_l $(j+1 \leqslant l \leqslant q)$ occurring in the walk W are contained in the set*

$$S_1 = \big\{(0,0,0,0), (0,0,1,0), (0,1,0,0), (1,0,0,0), (0,1,0,1)\big\}; \tag{20}$$

(ii) *if* $\omega = -1$, *all vertices* P_l $(j+1 \leqslant l \leqslant q)$ *occurring in the walk* W *are contained in the set*

$$S_2 = S_1 \cup \big\{(0,0,0,1), (0,0,1,1), (1,0,0,1)\big\}; \tag{21}$$

(iii) *if* $\omega = -2$, *all vertices* P_l $(j+1 \leqslant l \leqslant q)$ *occurring in the walk* W *are contained in the set*

$$S_3 = S_2 \cup \big\{(1,0,1,1), (0,1,1,1), (1,1,0,1)\big\}. \tag{22}$$

The proof of Lemma 6 is presented in Appendix B.

Lemma 7. *For the walk*

$$W\colon \quad P_0 \to P_1 \to \cdots \to P_{q-1} \to P_q$$

in the set $\mathcal{P}$, *if the initial vertex* $P_0 \in \{(1,0,0,0), (0,1,0,0), (0,0,1,0), (1,0,1,1), (1,1,0,1), (0,1,1,1)\}$, *then* W *cannot be closed.*

Proof. Let ϑ_j denote the arc with the tail P_j and head P_{j+1} for each $j \in \{0,1,\ldots,q-1\}$. Since $W \in \mathcal{P}$, by property (III) of the walks in $\mathcal{P}$, we have $w(\vartheta_0) \geqslant 2$. If W is closed, then we must have $P_q = P_0$ and $P_{q-1}(3) = P_1(2)$. The lemma is proven according to six cases of the vertex P_0 as follows.

If $P_0 = (1,0,0,0)$ and $w(\vartheta_0) \geqslant 2$, then $P_1 = (0,1,0,0)$ by Appendix A. Consequently, $P_2(2) = 0$ and by property (III) of the walks in $\mathcal{P}$, $w(\vartheta_1) \geqslant 1$. By a similar analysis as in Example 1, $(0,1,0,0) \xrightarrow{(0,1)}$ has an SBS as

$$(0,1,0,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(0,1)} \begin{cases} (1,0,0,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(0,1)} \\ (0,0,1,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(1,1)} (0,1,0,0) \xrightarrow{(0,1)}. \end{cases} \tag{23}$$

From (23), we can know that all vertices and arcs in $P_1 W P_q$ have occurred in (23). If $P_q = P_0 = (1,0,0,0)$, then by (23), $P_{q-1} = (0,0,0,0)$ and then $P_{q-1}(3) = 0 \neq P_1(2)$. Therefore the walk W cannot be closed if $P_0 = (1,0,0,0)$.

The case $P_0 = (0,1,0,0)$ can be similarly proven as the case $P_0 = (1,0,0,0)$.

If $P_0 = (0,0,1,0)$, then $P_0 W P_4$ has the form as

$$(0,0,1,0) \xrightarrow{(-,2)} (0,1,0,0) \xrightarrow{(1,1)} (0,1,0,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(0,0)}. \tag{24}$$

If W is closed, then $P_q = (0,0,1,0)$ and $P_{q-1}(3) = 1$. By (24), we have $q \geqslant 5$. By Lemma 6(i), the vertices P_j for $4 \leqslant j \leqslant q$ in W are contained in S_1. Consequently, $P_{q-1} \in S_1$. Notice that $(0,0,1,0)$ is the unique vertex with the third component 1 in the set S_1. As a consequence, $P_{q-1} = (0,0,1,0)$ and the arc ϑ_{q-1} is $(0,0,1,0) \to (0,0,1,0)$, which does not exist by Appendix A. This leads to a contradiction and then W cannot be closed.

If $P_0 = (1,0,1,1)$, then $(1,0,1,1) \xrightarrow{(-,2)}$ has an SBS as

$$(1,0,1,1) \xrightarrow{(-,2)} \begin{cases} (1,0,0,0) \xrightarrow{(1,1)} (0,1,0,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(0,0)} \\ (0,1,0,0) \xrightarrow{(1,1)} (0,1,0,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(0,0)} \\ (0,0,1,0) \xrightarrow{(1,1)} (0,1,0,0) \xrightarrow{(1,0)} (0,1,0,0) \xrightarrow{(0,-1)} (0,0,0,0) \xrightarrow{(0,-1)}. \end{cases} \tag{25}$$

The vertices P_j for $4 \leqslant j \leqslant q$ of the first and second segments of (25) are contained in S_1 and the vertices P_j for $5 \leqslant j \leqslant q$ of the third segment in (25) are contained in S_2 by Lemma 6(i) and (ii). Notice that $(1,0,1,1) \notin S_1$ and $(1,0,1,1) \notin S_2$. Consequently, the walk W cannot be closed.

Table 5
All arcs ϑ with $w(\vartheta) \geqslant 2$, $T(\vartheta) \notin S_3$ and $H(\vartheta) \notin \Gamma$.

$T(\vartheta)$	$H(\vartheta)$	$w(\vartheta)$	$T(\vartheta)$	$H(\vartheta)$	$w(\vartheta)$
(1, 1, 0, 2)	(1, 1, 1, 1)	2	(1, 0, 1, 2)	(1, 1, 1, 1)	2
(0, 1, 1, 2)	(1, 1, 1, 1)	2	(1, 1, 1, 3)	(1, 1, 1, 1)	2
(1, 1, 1, 1)	(0, 0, 0, 0)	2	(1, 1, 1, 1)	(0, 1, 0, 0)	3
(1, 1, 1, 2)	(1, 1, 0, 1)	2	(1, 1, 1, 2)	(0, 1, 1, 1)	2
(1, 1, 1, 2)	(1, 0, 0, 0)	2	(1, 1, 1, 2)	(0, 0, 1, 0)	2

Table 6
All arcs ϑ with $w(\vartheta) \geqslant 2$, $T(\vartheta) \in S_3$ and $H(\vartheta) \notin \Gamma$.

$T(\vartheta)$	$H(\vartheta)$	$w(\vartheta)$	$T(\vartheta)$	$H(\vartheta)$	$w(\vartheta)$
(1, 0, 0, 0)	(0, 1, 0, 0)	2	(0, 1, 0, 0)	(0, 1, 0, 0)	2
(0, 0, 1, 0)	(0, 1, 0, 0)	2	(1, 0, 1, 1)	(1, 0, 0, 0)	2
(1, 0, 1, 1)	(0, 1, 0, 0)	2	(1, 0, 1, 1)	(0, 0, 1, 0)	2
(1, 1, 0, 1)	(1, 0, 0, 0)	2	(1, 1, 0, 1)	(0, 1, 0, 0)	2
(1, 1, 0, 1)	(0, 0, 1, 0)	2	(0, 1, 1, 1)	(1, 0, 0, 0)	2
(0, 1, 1, 1)	(0, 1, 0, 0)	2	(0, 1, 1, 1)	(0, 0, 1, 0)	2

The cases $P_0 = (1, 1, 0, 1)$ and $(0, 1, 1, 1)$ can be similarly proven as the case $P_0 = (1, 0, 1, 1)$. The proof is finished. □

By Lemmas 6 and 7, we will finish the proof of Proposition 3 as below.

Proof of Proposition 3. If the result is not true, the walk W_0 defined in (15) belongs to the set $\mathcal{P}$ and $w(\vartheta_0) \geqslant 2$. We will prove that W_0 cannot be closed according to ϑ_0.

Notice that there are no arcs ϑ with tail $T(\vartheta) \in \Gamma$, where Γ is defined by (13). Consequently, W_0 cannot be closed if the head $H(\vartheta_0) \in \Gamma$. Therefore, we only need to consider the arcs ϑ_0 with $w(\vartheta_0) \geqslant 2$ and $H(\vartheta_0) \notin \Gamma$, i.e., the arcs listed in Tables 5 and 6, where S_3 is defined by (22).

To prove that $W_0 \in \mathcal{P}$ is not closed for any arc ϑ_0 in Table 5, we firstly present an SBS of the arc ϑ_0, then we have $P_j \neq P_0$ for $j \geqslant 1$ by Lemma 6. Since the arc ϑ_0 in Table 5 can be similarly proven, here we only present the proof of the arc $(1, 1, 1, 2) \to (0, 1, 1, 1)$, for simplicity.

By a similar analysis as Example 1, $(0, 1, 1, 1) \xrightarrow{(1,1)}$ has an SBS as

$$(0,1,1,1) \xrightarrow{(1,1)} \begin{cases} (0,1,0,0) \xrightarrow{(1,0)} (0,1,0,0) \xrightarrow{(0,-1)} (0,0,0,0) \xrightarrow{(0,-1)} \\ (0,1,0,1) \xrightarrow{(1,1)} \begin{cases} (1,1,0,1) \xrightarrow{(0,1)} \\ (0,1,1,1) \xrightarrow{(0,1)} . \end{cases} \end{cases}$$

The walks $(0, 1, 1, 1) \xrightarrow{(0,1)}$ and $(1, 1, 0, 1) \xrightarrow{(0,1)}$ have been analyzed in (B.7) and (B.8) in Appendix B, respectively. Thus by Lemma 6, the vertices P_j for $j \geqslant 1$ are contained in S_3. So W_0 cannot be closed since $(1, 1, 1, 2) \notin S_3$.

Suppose that ϑ_0 satisfies $T(\vartheta_0) \in S_3$ and $H(\vartheta_0) \notin \Gamma$, i.e., those arcs in Table 6. By Lemma 7, we still have that the walk W_0 cannot be closed for any ϑ_0 given by Table 6. However, by (11) and the analysis therein, we have that W_0 is closed. This contradiction shows that the assumption at the beginning of the proof does not hold, and then the proof is finished. □

Remark 3. (1) In the proof of Proposition 3, we do not distinguish whether the vertices of the walk W_0 are in the set $\{V_0, V_1, \ldots, V_{m-1}\}$ or not. That is to say, we have proven that each walk in $\mathcal{P}$ cannot be closed.

(2) In the papers [16,17], the authors defined an equivalence relation (i.e., two vertices are called *equivalent* if there exists a closed walk in directed graph $\mathbb{D}$ containing both these vertices), and determined the equivalence classes (called *strongly connected components*) by computer. However, in this

paper, the property (II) should be considered to prove Proposition 3 and we don't find a suitable method to define a similar equivalence relation which can be efficiently checked by computer.

Proposition 4. *For the integer sequence $\nu_0, \nu_1, \ldots, \nu_{m-1}$ of period m, if for any $\nu_i \geqslant 2$, there exists a positive integer $t_i \leqslant m$ such that*

$$\nu_i + \nu_{i-1} + \cdots + \nu_{i-t_i+1} \leqslant t_i, \tag{26}$$

then $\sum_{i=0}^{m-1} \nu_i \leqslant m$.

Proof. Without loss of generality, we can assume that the integer t_i is the smallest integer such that (26) holds.

Let $I = \{i \mid \nu_i \geqslant 2\}$ and $|I| = p$. Thus, all elements of I can be listed as $i_1, i_2, \ldots, i_p$, where $i_1 < i_2 < \cdots < i_p$. Let $N_j = \{i_j, i_j - 1, \ldots, i_j - t_{i_j} + 1\}$ be a subset of $\mathbb{Z}_m$. Then (26) can be written as $\sum_{i \in N_j} \nu_i \leqslant t_{i_j} = |N_j|$. Let $N = \bigcup_{j=1}^{p} N_j$, and then $\nu_i \leqslant 1$ if $i \in \mathbb{Z}_m \setminus N$.

If $p = 1$, $\nu_{i_1} + \nu_{i_1-1} + \cdots + \nu_{i_1-t_1+1} \leqslant t_{i_1}$. In this case, the proof follows the fact that other ν_j satisfies $\nu_j \leqslant 1$.

If $p \geqslant 2$, we claim that for two integers j and j' with $1 \leqslant j < j' \leqslant p$, the sets N_j and $N_{j'}$ are disjoint or one containing another one. Without loss of generality, we take $j = 1$ and $j' = 2$.

If the above claim is not true, then we have $i_1 - t_{i_1} + 1 < i_2 - t_{i_2} + 1 \leqslant i_1 < i_2$ and consider the following sequence

$$\nu_{i_1-t_{i_1}+1}, \ldots, \nu_{i_2-t_{i_2}+1}, \nu_{i_2-t_{i_2}+2}, \ldots, \nu_{i_1}, \ldots, \nu_{i_2}.$$

Notice that t_{i_1} and t_{i_2} are the smallest positive integers satisfying (26). Consequently, we have

$$\nu_{i_2-t_{i_2}+1} + \nu_{i_2-t_{i_2}+2} + \cdots + \nu_{i_1} > i_1 - i_2 + t_{i_2} \quad \text{and} \quad \nu_{i_1+1} + \nu_{i_1+2} + \cdots + \nu_{i_2} > i_2 - i_1.$$

This implies

$$\nu_{i_2-t_2+1} + \nu_{i_2-t_2+2} + \cdots + \nu_{i_1} + \nu_{i_1+1} + \nu_{i_1+2} + \cdots + \nu_{i_2} > t_{i_2},$$

which contradicts with (26) and then the claim is true. Thus there exists a subset J of the set $\{1, 2, \ldots, p\}$ such that $N = \bigcup_{j \in J} N_j$ and $N_j \cap N_{j'} = \emptyset$ for any two different elements j and j' of J. Thus $|N| = \sum_{j \in J} |N_j| = \sum_{j \in J} t_{i_j}$ and we have that $\sum_{i \in N} \nu_i = \sum_{j \in J} \sum_{i \in N_j} \nu_i \leqslant \sum_{j \in J} t_{i_j} = |N|$. Therefore, we have

$$\sum_{i=0}^{m-1} \nu_i = \sum_{i \in \mathbb{Z}_m \setminus N} \nu_i + \sum_{i \in N} \nu_i \leqslant \sum_{i \in \mathbb{Z}_m \setminus N} 1 + |N| = m,$$

and this finishes the proof. □

Propositions 3 and 4 tell us that $M(m; 3, 13) \leqslant k$. Furthermore, we can also prove that the equal sign holds.

Lemma 8. *(See [17, Theorem 14].) If $m/(m, r)$ is odd, then we have that*

$$M\big(m; 2^r + 1\big) = \big(m - (m, r)\big)/2.$$

Proof of Proposition 2. By Propositions 3 and 4, we have $w(\nu) \leqslant m$ and then by (9)

$$M(m;3,13) = \max\big(w(s) - w(a) - w(b)\big) \leqslant k$$

where the maximum is over all integers s, a, b such that

$$0 \leqslant s, a, b \leqslant 2^m - 1, \qquad s \equiv 3a + 13b \pmod{2^m - 1}, \qquad a \text{ or } b \not\equiv 0 \pmod{2^m - 1}.$$

On the other hand, we have $M(m;3,13) \geqslant M(m;3)$ by the definition of $M(m;3,13)$. Applying Lemma 8, we have

$$k = \big(m - (m,r)\big)/2 = M(m;3) \leqslant M(m;3,13) \leqslant k.$$

Therefore, we have $M(m;3,13) = k$ and the proof is finished. □

Remark 4. (1) For the power function $f(x) = x^{\frac{13}{3}}$ over $\mathbb{F}_{2^m}$, the Fourier coefficients $\widehat{f_{\frac{13}{3}}}(\gamma) = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m(x^{\frac{13}{3}}+\gamma x)}$ ($\gamma \in \mathbb{F}_{2^m}$) were considered and val($\frac{13}{3}$) was determined in Ref. [21], where val($\frac{13}{3}$) is the largest integer d such that 2^d divides all the Fourier coefficients $\widehat{f_{\frac{13}{3}}}(\gamma)$. Notice that $\gcd(3, 2^m - 1) = 1$ and then $\sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m(x^{\frac{13}{3}}+\gamma x)} = \sum_{x\in\mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_1^m(x^{13}+\gamma x^3)}$. With the notations as in equality (1), let $d_1 = 3$ and $d_2 = 13$, and then we have

$$\widehat{f_{\frac{13}{3}}}(\gamma) = 2^m - 2\,wt\big(\mathbf{c}(0,\gamma,1)\big) \tag{27}$$

where $\mathbf{c}(0,\gamma,1)$ is a codeword in $\mathcal{C}^{\perp}_{1,3,13}$. By Theorem 1 and the weights of codewords in $\mathcal{C}^{\perp}_{1,3,5}$, $\widehat{f_{\frac{13}{3}}}(\gamma)$ has at most five possible values as in the set $\{0, \pm 2^{\frac{m+1}{2}}, \pm 2^{\frac{m+3}{2}}\}$ and then val($\frac{13}{3}$) $\geqslant \frac{m+1}{2}$. Assume that τ is the largest integer such that $2^\tau \mid wt(\mathbf{c}(0,\gamma,1))$ for all $\gamma \in \mathbb{F}_{2^m}$. Then we have val($\frac{13}{3}$) $= \tau + 1$ according to the equality (27). We also have $\tau \geqslant M(m;3,13)$, since the set consisting of the codewords $wt(\mathbf{c}(0,\gamma,1))$ with $\gamma \in \mathbb{F}_{2^m}$ is a subset of the code $\mathcal{C}^{\perp}_{1,3,13}$. Thus, we can obtain the same conclusion that val($\frac{13}{3}$) $\geqslant M(m;3,13) + 1 = \frac{m+1}{2}$ by Proposition 2.

(2) Ref. [21] utilized the Gauss sums and Stickelberger's congruences to obtain the inequality

$$\mathrm{val}(13/3) \geqslant \min_{1\leqslant a\leqslant 2^m-2} \big\{wt(-a) + wt(13a/3)\big\} = \min_{1\leqslant a\leqslant 2^m-2} \big\{wt(-3a) + wt(13a)\big\},$$

and then applied the add-with-carry algorithm to 3 and 13, respectively. By constructing a weighted graph of 96 vertices and then simplifying this graph to a weighted graph of 44 vertices, Leander and Langevin [21] enumerated all elementary cycles in the simplified graph and found that the costs (i.e., weights) of elementary cycles of length $2L$ or $2L+1$ are greater or equal to $-L$ (computer checking). This shows val($\frac{13}{3}$) $\geqslant \frac{m+1}{2}$. In our paper, the method introduced in Section 2 (also see Ref. [16]) is used to determine the value of $M(m;3,13)$. We construct a weighted graph of 40 vertices and analyze the maximum value of $M(m;3,13)$ according to Steps 1 and 2 (the arcs and their weights in the graph defined in our paper are also found by a computer, but our proofs are finished by hand).

(3) For $m = 2k+1$, to determine the largest power of 2 dividing all weights of the cyclic code $\mathcal{C}^{\perp}_{1,2^{k+1}+1,2^{k+2}+3}$, Hollmann and Xiang applied the add-with-carry algorithm to prove $M(m; 2^{k+1} - 1, 2^{k+1} + 1) \leqslant \frac{m-1}{2}$ [16] since $\mathcal{C}^{\perp}_{1,2^{k+1}+1,2^{k+2}+3}$ and $\mathcal{C}^{\perp}_{1,2^{k+1}-1,2^{k+1}+1}$ have the same weight distribution.

To the end, the authors needed to use the equalities

$$2c_i + s_i = a_{i-k-1} - a_i + b_{i-k-1} + b_i + c_{i-1} \tag{28}$$

for all $i \in \mathbb{Z}_m$ in the Appendix of [16]. Since $m = 2k+1$, the following useful equalities

$$2c_{i-k-1} + s_{i-k-1} = a_{i-1} - a_{i-k-1} + b_{i-1} + b_{i-k-1} + c_{i-k-2} \tag{29}$$

can be derived from (28) by replacing i by $i-k-1$, where the subscripts are taken modulo m. With these equalities, the authors constructed a directed graph and analyzed the five arcs of weight 2 in its component G_0 to prove $M(m; 2^{k+1}-1, 2^{k+1}+1) \leqslant \frac{m-1}{2}$ (see the Appendix of [16] for details). However, we do not find any useful relationship between the subscripts in (6) and k. Therefore, we do not obtain the equalities as (29), and a special set $\mathcal{P}$ as in (14) is defined to prove $M(m; 3, 13) \leqslant \frac{m-1}{2}$. This makes the divisibility analysis in this paper more complex than that of the cyclic code $\mathcal{C}^{\perp}_{1,2^{k+1}+1,2^{k+2}+3}$ in [16] although the pair (3, 13) is fixed and independent on m.

5. Conclusions

For odd $m \geqslant 5$, a new triple-error-correcting cyclic code of length $2^m - 1$ has been found. It is defined by zeros α, α^3 and α^{13}, and the exponents 3 and 13 come from the Gold and Kasami–Welch APN power functions, respectively. To generalize the construction of the code $\mathcal{C}_{1,3,13}$, one can consider the class of cyclic codes $\mathcal{C}$ with the dual codes $\mathcal{C}^{\perp}$ having the form

$$\mathcal{C}^{\perp} = \left\{ \mathbf{c}(\epsilon, \gamma, \delta) = \left(\mathrm{Tr}_1^m\left(\epsilon x + \gamma f(x) + \delta g(x)\right)\right)_{x \in \mathbb{F}_{2^m}^*} \;\middle|\; \epsilon, \gamma, \delta \in \mathbb{F}_{2^m} \right\}$$

where $f(x)$ and $g(x)$ are different APN functions from $\mathbb{F}_{2^m}$ to itself. If the polynomial $\mathrm{Tr}_1^m(\epsilon x + \gamma f(x) + \delta g(x))$ in variable x has algebraic degree greater than 2, some tools other than the theory of quadratic forms are possibly needed.

Acknowledgments

The authors would like to thank the editor and the two anonymous reviewers for their helpful comments, and they are indebted to one reviewer for pointing out the relation between the divisibility analysis in this paper and that in [21], which have improved the presentation of this paper. The first author would like to thank Qing Xiang for his encouragement and Gregor Leander for sending him the preprint of [21].

Appendix A. Some arcs ϑ in $\mathbb{D}$

Appendix A gives all arcs ϑ with the head $H(\vartheta) \notin \Gamma$ and tail $T(\vartheta)$ in the set

$$S_3 \cup \left\{(1,1,0,2), (1,0,1,2), (0,1,1,2), (1,1,1,1)\right\},$$

where the set S_3 is defined as (22).

1. $T(\vartheta) = (0,0,0,0)$.

$H(\vartheta)$	$(0,0,0,0)$	$(0,0,0,1)$	$(1,0,0,0)$	$(0,1,0,0)$	$(0,1,0,1)$	$(0,0,1,0)$
$w(\vartheta)$	0	-1	1	1	0	1

2. $T(\vartheta) = (0, 0, 0, 1)$.

$H(\vartheta)$	$(0, 0, 0, 2)$	$(0, 0, 0, 3)$	$(1, 0, 0, 1)$	$(1, 0, 0, 2)$	$(0, 1, 0, 2)$
$w(\vartheta)$	-3	-4	-1	-2	-2
$H(\vartheta)$	$(0, 1, 0, 3)$	$(1, 1, 0, 1)$	$(1, 1, 0, 2)$	$(0, 0, 1, 1)$	$(0, 0, 1, 2)$
$w(\vartheta)$	-3	0	-1	-1	-2
$H(\vartheta)$	$(1, 0, 1, 1)$	$(0, 1, 1, 1)$	$(0, 1, 1, 2)$	$(1, 1, 1, 1)$	
$w(\vartheta)$	0	0	-1	1	

3. $T(\vartheta) = (1, 0, 0, 0)$.

$H(\vartheta)$	$(0, 0, 0, 0)$	$(0, 1, 0, 0)$
$w(\vartheta)$	1	2

4. $T(\vartheta) = (1, 0, 0, 1)$.

$H(\vartheta)$	$(0, 0, 0, 1)$	$(0, 0, 0, 2)$	$(1, 0, 0, 0)$	$(1, 0, 0, 1)$	$(0, 1, 0, 1)$
$w(\vartheta)$	-1	-2	1	0	0
$H(\vartheta)$	$(0, 1, 0, 2)$	$(1, 1, 0, 1)$	$(0, 0, 1, 0)$	$(0, 0, 1, 1)$	$(0, 1, 1, 1)$
$w(\vartheta)$	-1	1	1	0	1

5. $T(\vartheta) = (0, 1, 0, 0)$.

$H(\vartheta)$	$(0, 0, 0, 0)$	$(0, 1, 0, 0)$
$w(\vartheta)$	1	2

6. $T(\vartheta) = (0, 1, 0, 1)$.

$H(\vartheta)$	$(0, 0, 0, 1)$	$(0, 0, 0, 2)$	$(1, 0, 0, 0)$	$(1, 0, 0, 1)$	$(0, 1, 0, 1)$
$w(\vartheta)$	-1	-2	1	0	0
$H(\vartheta)$	$(0, 1, 0, 2)$	$(1, 1, 0, 1)$	$(0, 0, 1, 0)$	$(0, 0, 1, 1)$	$(0, 1, 1, 1)$
$w(\vartheta)$	-1	1	1	0	1

7. $T(\vartheta) = (1, 1, 0, 1)$.

$H(\vartheta)$	$(0, 0, 0, 0)$	$(0, 0, 0, 1)$	$(1, 0, 0, 0)$	$(0, 1, 0, 0)$	$(0, 1, 0, 1)$	$(0, 0, 1, 0)$
$w(\vartheta)$	1	0	2	2	1	2

8. $T(\vartheta) = (1, 1, 0, 2)$.

$H(\vartheta)$	$(0, 0, 0, 2)$	$(0, 0, 0, 3)$	$(1, 0, 0, 1)$	$(1, 0, 0, 2)$	$(0, 1, 0, 2)$
$w(\vartheta)$	-2	-3	0	-1	-1
$H(\vartheta)$	$(0, 1, 0, 3)$	$(1, 1, 0, 1)$	$(1, 1, 0, 2)$	$(0, 0, 1, 1)$	$(0, 0, 1, 2)$
$w(\vartheta)$	-2	1	0	0	-1
$H(\vartheta)$	$(1, 0, 1, 1)$	$(0, 1, 1, 1)$	$(0, 1, 1, 2)$	$(1, 1, 1, 1)$	
$w(\vartheta)$	1	1	0	2	

9. $T(\vartheta) = (0, 0, 1, 0)$.

$H(\vartheta)$	$(0, 0, 0, 0)$	$(0, 1, 0, 0)$
$w(\vartheta)$	1	2

10. $T(\vartheta) = (0, 0, 1, 1)$.

$H(\vartheta)$	$(0, 0, 0, 1)$	$(0, 0, 0, 2)$	$(1, 0, 0, 0)$	$(1, 0, 0, 1)$	$(0, 1, 0, 1)$
$w(\vartheta)$	-1	-2	1	0	0
$H(\vartheta)$	$(0, 1, 0, 2)$	$(1, 1, 0, 1)$	$(0, 0, 1, 0)$	$(0, 0, 1, 1)$	$(0, 1, 1, 1)$
$w(\vartheta)$	-1	1	1	0	1

11. $T(\vartheta) = (1, 0, 1, 1)$.

$H(\vartheta)$	$(0, 0, 0, 0)$	$(0, 0, 0, 1)$	$(1, 0, 0, 0)$	$(0, 1, 0, 0)$	$(0, 1, 0, 1)$	$(0, 0, 1, 0)$
$w(\vartheta)$	1	0	2	2	1	2

12. $T(\vartheta) = (1, 0, 1, 2)$.

$H(\vartheta)$	$(0, 0, 0, 2)$	$(0, 0, 0, 3)$	$(1, 0, 0, 1)$	$(1, 0, 0, 2)$	$(0, 1, 0, 2)$
$w(\vartheta)$	-2	-3	0	-1	-1
$H(\vartheta)$	$(0, 1, 0, 3)$	$(1, 1, 0, 1)$	$(1, 1, 0, 2)$	$(0, 0, 1, 1)$	$(0, 0, 1, 2)$
$w(\vartheta)$	-2	1	0	0	-1
$H(\vartheta)$	$(1, 0, 1, 1)$	$(0, 1, 1, 1)$	$(0, 1, 1, 2)$	$(1, 1, 1, 1)$	
$w(\vartheta)$	1	1	0	2	

13. $T(\vartheta) = (0, 1, 1, 1)$.

$H(\vartheta)$	$(0, 0, 0, 0)$	$(0, 0, 0, 1)$	$(1, 0, 0, 0)$	$(0, 1, 0, 0)$	$(0, 1, 0, 1)$	$(0, 0, 1, 0)$
$w(\vartheta)$	1	0	2	2	1	2

14. $T(\vartheta) = (0, 1, 1, 2)$.

$H(\vartheta)$	$(0, 0, 0, 2)$	$(0, 0, 0, 3)$	$(1, 0, 0, 1)$	$(1, 0, 0, 2)$	$(0, 1, 0, 2)$
$w(\vartheta)$	-2	-3	0	-1	-1
$H(\vartheta)$	$(0, 1, 0, 3)$	$(1, 1, 0, 1)$	$(1, 1, 0, 2)$	$(0, 0, 1, 1)$	$(0, 0, 1, 2)$
$w(\vartheta)$	-2	1	0	0	-1
$H(\vartheta)$	$(1, 0, 1, 1)$	$(0, 1, 1, 1)$	$(0, 1, 1, 2)$	$(1, 1, 1, 1)$	
$w(\vartheta)$	1	1	0	2	

15. $T(\vartheta) = (1, 1, 1, 1)$.

$H(\vartheta)$	$(0, 0, 0, 0)$	$(0, 1, 0, 0)$
$w(\vartheta)$	2	3

Appendix B. Proof of Lemma 6

Proof. The proofs of Lemma 6(i) and (ii) are contained in the proof of Lemma 6(iii), so we only focus on the proof for (iii). Furthermore, from the SBS (B.6), we will see that the case $P_{j+1}(2) = 1$ and $\omega = -2$ is contained in the case $P_{j+1}(2) = 0$ and $\omega = -2$, thus we always assume that $P_{j+1}(2) = 0$ and $\omega = -2$ in the sequel. For the same reason as in Example 1, without loss of generality, we can also assume that the integer q is large enough.

Let ϑ_i denote the arc with the tail P_i and head P_{i+1} for $0 \leqslant i \leqslant q-1$.

Since $P_{j+1}(2) = 0$ and $\omega = -2$, by $P_j = (0,0,0,0)$ and Appendix A, we have $P_{j+1} \in \{(0,0,0,0), (0,0,0,1), (0,0,1,0), (1,0,0,0)\}$. If $P_{j+1} = (0,0,0,0)$, then $w(\vartheta_j) = 0$. By a similar analysis as in (16), we have $w(\vartheta_{j+1}) \geqslant -1$. Consequently, $P_j W P_{j+2}$ has the form as

$$(0,0,0,0) \xrightarrow{(0,-2)} (0,0,0,0) \xrightarrow{(0,-1)} \qquad (\Phi 1). \tag{B.1}$$

For $P_{j+1} \in \{(0,0,0,1), (0,0,1,0), (1,0,0,0)\}$, a similar analysis shows that $P_j W P_{j+2}$ has other three possible forms as below.

$$(0,0,0,0) \xrightarrow{(0,-2)} \begin{cases} (0,0,0,1) \xrightarrow{(0,0)} & (\Phi 2) \\ (0,0,1,0) \xrightarrow{(0,-2)} & (\Phi 3) \\ (1,0,0,0) \xrightarrow{(0,-2)} & (\Phi 4). \end{cases}$$

In the case $(\Phi 1)$, $P_{j+2}(2) = 0$ and then by Appendix A, we have

$$P_{j+2} \in \big\{(0,0,0,0), (0,0,0,1), (0,0,1,0), (1,0,0,0)\big\}.$$

Notice that the weights of the arcs with the tail P_{j+1} and heads $(0,0,0,0)$, $(0,0,0,1)$, $(0,0,1,0)$, $(1,0,0,0)$ are 0, -1, 1, 1, respectively. Consequently, there are four possible forms for $P_j W P_{j+3}$ as

$$(0,0,0,0) \xrightarrow{(0,-2)} (0,0,0,0) \xrightarrow{(0,-1)} \begin{cases} (0,0,0,0) \xrightarrow{(0,0)} & (\Phi 1.1) \\ (0,0,0,1) \xrightarrow{(0,1)} & (\Phi 1.2) \\ (0,0,1,0) \xrightarrow{(0,-1)} & (\Phi 1.3) \\ (1,0,0,0) \xrightarrow{(0,-1)} & (\Phi 1.4). \end{cases}$$

For the case $(\Phi 1.1)$, by a similar analysis as Example 1, the walk $(0,0,0,0) \xrightarrow{(0,0)}$ has an SBS as

$$(0,0,0,0) \xrightarrow{(0,0)} \begin{cases} (0,0,0,0) \xrightarrow{(0,1)} \begin{cases} (0,0,1,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(1,1)} (0,1,0,0) \\ \quad \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(0,1)} \\ (1,0,0,0) \xrightarrow{(0,1)} (0,0,0,0) \xrightarrow{(0,1)} \end{cases} \\ (0,0,1,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(1,0)} \begin{cases} (0,1,0,1) \xrightarrow{(0,1)} \begin{cases} (0,0,1,0) \xrightarrow{(0,1)} \\ (1,0,0,0) \xrightarrow{(0,1)} \end{cases} \\ (0,1,0,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(0,0)} \end{cases} \\ (1,0,0,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(0,0)}, \end{cases} \tag{B.2}$$

in which all vertices and arcs in $P_{j+2} W P_q$ have occurred for the case $P_{j+2} = (0,0,0,0)$. Thus, all vertices P_l $(j+1 \leqslant l \leqslant q)$ occurring in the walk W are contained in the set S_1 defined by (20). Furthermore, by (B.2), all walks with the form $(0,0,0,0) \xrightarrow{(\eta,\omega)}$ for $\eta \in \{0,1\}$ and $\omega \in \{0,1\}$ have occurred in (B.2). This finishes the proof of Lemma 6(i).

For the case $(\Phi 1.2)$, by Appendix A, we have $(0,0,0,1) \xrightarrow{(0,1)} O$, i.e., $q = j+2$ and $P_{j+2} = P_q$.

For the case (Φ1.3), $P_{j+2}WP_{j+6}$ has five possible forms as

$$(0,0,1,0)\xrightarrow{(0,-1)}(0,0,0,0)\xrightarrow{(1,-1)}\begin{cases}(0,1,0,0)\xrightarrow{(0,-1)}(0,0,0,0)\xrightarrow{(0,-1)} & (\Phi 1.3.1)\\ (0,1,0,1)\xrightarrow{(0,0)}\begin{cases}(0,0,1,0)\xrightarrow{(0,0)} & (\Phi 1.3.2)\\ (0,0,1,1)\xrightarrow{(0,1)} & (\Phi 1.3.3)\\ (1,0,0,0)\xrightarrow{(0,0)} & (\Phi 1.3.4)\\ (1,0,0,1)\xrightarrow{(0,1)} & (\Phi 1.3.5).\end{cases}\end{cases} \tag{B.3}$$

The walks $(0,0,1,0)\xrightarrow{(0,0)}$ in (Φ1.3.2) and $(1,0,0,0)\xrightarrow{(0,0)}$ in (Φ1.3.4) have occurred in (B.2). We need to further analyze the cases (Φ1.3.3) and (Φ1.3.5). By Appendix A, $(0,0,1,1)\xrightarrow{(0,1)}$ has an SBS as

$$(0,0,1,1)\xrightarrow{(0,1)}\begin{cases}(0,0,1,0)\xrightarrow{(1,1)}(0,1,0,0)\xrightarrow{(1,0)}(0,1,0,0)\xrightarrow{(0,-1)}(0,0,0,0)\xrightarrow{(0,-1)}\\ (1,0,0,0)\xrightarrow{(1,1)}(0,1,0,0)\xrightarrow{(0,0)}(0,0,0,0)\xrightarrow{(0,0)}\end{cases} \tag{B.4}$$

for the case (Φ1.3.3) and $(1,0,0,1)\xrightarrow{(0,1)}$ has an SBS as

$$(1,0,0,1)\xrightarrow{(0,1)}\begin{cases}(0,0,1,0)\xrightarrow{(0,1)}(0,0,0,0)\xrightarrow{(1,1)}\\ (1,0,0,0)\xrightarrow{(0,1)}(0,0,0,0)\xrightarrow{(0,1)}\end{cases} \tag{B.5}$$

for the case (Φ1.3.5).

For the case (Φ1.4), $P_{j+2}WP_{j+4}$ is given by

$$(1,0,0,0)\xrightarrow{(0,-1)}(0,0,0,0)\xrightarrow{(0,-1)}.$$

Notice that the walk $(0,0,0,0)\xrightarrow{(0,-1)}$ in (Φ1.3.1), (Φ1.3.3) and (Φ1.4) has occurred as $P_{j+1}WP_{j+2}$ in (B.1). Therefore, by the above analysis for (Φ1.1)–(Φ1.4) and Lemma 6(i), in the case that P_jWP_{j+2} has the form as (B.1), all vertices P_l $(j+1\leqslant l\leqslant q)$ occurring in the walk W are contained in the set S_2 defined by (21). Furthermore, the walks $(0,0,0,0)\xrightarrow{(\eta,-1)}$ for $\eta\in\{0,1\}$ have occurred in (B.3). This finishes the proof of Lemma 6(ii).

For the case (Φ2), $(0,0,0,1)\xrightarrow{(0,0)}(1,0,1,1)$ has an SBS as

$$\begin{aligned}&(0,0,0,1)\xrightarrow{(0,0)}(1,0,1,1)\\ &\xrightarrow{(0,1)}\begin{cases}(0,0,0,0)\xrightarrow{(1,1)}\\ (0,0,1,0)\xrightarrow{(1,0)}(0,1,0,0)\xrightarrow{(1,-1)}(0,1,0,0)\xrightarrow{(0,-2)}(0,0,0,0)\xrightarrow{(0,-2)}\\ (1,0,0,0)\xrightarrow{(1,0)}(0,1,0,0)\xrightarrow{(0,-1)}(0,0,0,0)\xrightarrow{(0,-1)}.\end{cases}\end{aligned}$$

For the case (Φ3), $P_{j+1}WP_{j+5}$ has six possible forms as

$$\begin{aligned}&(0,0,1,0)\xrightarrow{(0,-2)}(0,0,0,0)\\ &\xrightarrow{(1,-2)}\begin{cases}(0,1,0,0)\xrightarrow{(0,-2)}(0,0,0,0)\xrightarrow{(0,-2)} & (\Phi 3.1)\\ (0,1,0,1)\xrightarrow{(0,-1)}\begin{cases}(0,0,0,1)\xrightarrow{(0,1)} & (\Phi 3.2)\\ (0,0,1,0)\xrightarrow{(0,-1)} & (\Phi 3.3)\\ (0,0,1,1)\xrightarrow{(0,0)} & (\Phi 3.4)\\ (1,0,0,0)\xrightarrow{(0,-1)} & (\Phi 3.5)\\ (1,0,0,1)\xrightarrow{(0,0)} & (\Phi 3.6).\end{cases}\end{cases}\end{aligned} \tag{B.6}$$

The walk $(0,0,0,1) \xrightarrow{(0,1)}$ in (Φ3.2) has occurred as $P_{j+2}WP_{j+3}$ in (Φ1.2). For the case (Φ3.3), since the segment $P_{j+4}WP_{j+5}$ has the form $(0,0,1,0) \xrightarrow{(0,-1)}$, the segment $P_{j+4}WP_{j+6}$ has the form $(0,0,1,0) \xrightarrow{(0,-1)} (0,0,0,0) \xrightarrow{(1,-1)}$. By Lemma 6(ii), for the cases (Φ3.2) and (Φ3.3), all vertices in W are contained in the set S_2.

For the case (Φ3.4), $(0,0,1,1) \xrightarrow{(0,0)}$ has an SBS as

$$(0,0,1,1) \xrightarrow{(0,0)} \begin{cases} (0,0,1,0) \xrightarrow{(1,0)} (0,1,0,0) \xrightarrow{(1,-1)} (0,1,0,0) \\ \quad \xrightarrow{(0,-2)} (0,0,0,0) \xrightarrow{(0,-2)} & (\Phi 3.4.1) \\ (0,0,1,1) \xrightarrow{(1,1)} \begin{cases} (1,1,0,1) \xrightarrow{(1,1)} & (\Phi 3.4.2) \\ (0,1,1,1) \xrightarrow{(1,1)} & (\Phi 3.4.3) \end{cases} \\ (1,0,0,0) \xrightarrow{(1,0)} (0,1,0,0) \xrightarrow{(0,-1)} (0,0,0,0) \xrightarrow{(0,-1)} & (\Phi 3.4.4) \\ (1,0,0,1) \xrightarrow{(1,1)} \begin{cases} (0,1,1,1) \xrightarrow{(0,1)} & (\Phi 3.4.5) \\ (1,1,0,1) \xrightarrow{(0,1)} & (\Phi 3.4.6). \end{cases} \end{cases}$$

For the case (Φ3.4.2), $(0,0,1,1) \xrightarrow{(1,1)}$ has an SBS as

$$(1,1,0,1) \xrightarrow{(1,1)} \begin{cases} (0,1,0,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(0,0)} \\ (0,1,0,1) \xrightarrow{(0,1)} \end{cases}$$

and the walk $(0,1,0,1) \xrightarrow{(0,1)}$ has occurred in (B.2). For the case (Φ3.4.3), $P_{j+6}WP_{j+9}$ has three possible forms as

$$(0,1,1,1) \xrightarrow{(1,1)} \begin{cases} (0,1,0,0) \xrightarrow{(1,0)} (0,1,0,0) \xrightarrow{(0,-1)} & (\Phi 3.4.3.1) \\ (0,1,0,1) \xrightarrow{(1,1)} \begin{cases} (0,1,1,1) \xrightarrow{(0,1)} & (\Phi 3.4.3.2) \\ (1,1,0,1) \xrightarrow{(0,1)} & (\Phi 3.4.3.3). \end{cases} \end{cases}$$

Since the walk $(0,1,0,0) \xrightarrow{(0,-1)}$ in the case (Φ3.4.3.1) has occurred in the case (Φ1.3.1) as (B.3), we need to further analyze the cases (Φ3.4.3.2) and (Φ3.4.3.3). $(0,1,1,1) \xrightarrow{(0,1)}$ has an SBS as

$$(0,1,1,1) \xrightarrow{(0,1)} \begin{cases} (0,0,0,0) \xrightarrow{(1,1)} \\ (0,0,1,0) \xrightarrow{(1,0)} (0,1,0,0) \xrightarrow{(1,-1)} (0,1,0,0) \xrightarrow{(0,-2)} (0,0,0,0) \xrightarrow{(0,-2)} \\ (1,0,0,0) \xrightarrow{(1,0)} (0,1,0,0) \xrightarrow{(0,-1)} (0,0,0,0) \xrightarrow{(0,-1)} \end{cases} \quad (B.7)$$

for (Φ3.4.3.2), and $(1,1,0,1) \xrightarrow{(0,1)}$ has an SBS as

$$(1,1,0,1) \xrightarrow{(0,1)} \begin{cases} (0,0,0,0) \xrightarrow{(0,1)} \\ (0,0,1,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(1,0)} \\ (1,0,0,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(0,0)} \end{cases} \quad (B.8)$$

for (Φ3.4.3.3).

Notice that the walk $(0,0,0,0) \xrightarrow{(0,-1)}$ in (Φ3.4.4) has occurred in (Φ1) and the walks $(0,1,1,1) \xrightarrow{(0,1)}$ in (Φ3.4.5) and $(1,1,0,1) \xrightarrow{(0,1)}$ in (Φ3.4.6) have been analyzed in (B.7) and (B.8), respectively.

For the case ($\Phi 3.5$), $P_{j+4}WP_{j+6}$ has the form as

$$(1,0,0,0) \xrightarrow{(0,-1)} (0,0,0,0) \xrightarrow{(0,-1)}$$

and for the case ($\Phi 3.6$), $(1,0,0,1) \xrightarrow{(0,0)}$ has an SBS as

$$(1,0,0,1) \xrightarrow{(0,0)} \begin{cases} (0,0,1,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(1,0)} \\ (0,0,1,1) \xrightarrow{(0,1)} \\ (1,0,0,0) \xrightarrow{(0,0)} (0,0,0,0) \xrightarrow{(0,0)} \\ (1,0,0,1) \xrightarrow{(0,1)} . \end{cases}$$

Notice that the walks $(0,0,1,1) \xrightarrow{(0,1)}$ and $(1,0,0,1) \xrightarrow{(0,1)}$ have been analyzed in (B.4) and (B.5), respectively.

For the case ($\Phi 4$), the segment $P_{j+1}WP_{j+3}$ has the form $(1,0,0,0) \xrightarrow{(0,-2)} (0,0,0,0) \xrightarrow{(0,-2)}$.

Notice that the walk $(0,0,0,0) \xrightarrow{(0,-2)}$ in the cases ($\Phi 2$), ($\Phi 3.1$), ($\Phi 3.4.1$), ($\Phi 3.4.3.2$), ($\Phi 3.4.5$), and ($\Phi 4$) has occurred as P_jWP_{j+1}. Therefore, combining the above analysis for the cases ($\Phi 2$)–($\Phi 4$) and by Lemma 6(i), (ii), all vertices P_l $(j+1 \leqslant l \leqslant q)$ occurring in the walk W are contained in the set S_3. The proof for the case $\eta = 1$ and $\omega = -2$ is contained in the analysis of the case ($\Phi 3$) in (B.6). This finishes the proof of Lemma 6(iii). □

References

[1] E. Berlekamp, Algebraic Coding Theory, McGraw–Hill, New York, 1968.
[2] E. Berlekamp, The weight enumerators for certain subcodes of the second order binary Reed–Muller codes, Inf. Contr. 17 (1970) 485–500.
[3] E. Berlekamp, Weight enumeration theorems, in: Proc. Sixth Allerton Conf. Circuit and Systems Theory, Urbana, IL, 1968, pp. 161–170.
[4] T. Beth, C. Ding, On almost perfect nonlinear permutations, in: Advances in Cryptography – EUROCRYPT'93, in: Lecture Notes in Comput. Sci., vol. 765, Springer-Verlag, Berlin, Germany, 1994, pp. 65–76.
[5] J. Bondy, U. Murty, Graph Theory, Springer-Verlag, Berlin, Germany, 2008.
[6] R. Bose, D. Ray-Chaudhuri, On a class of error correcting binary group codes, Inf. Contr. 3 (1960) 68–79.
[7] K. Browning, J. Dillon, R.E. Kibler, M. McQuistan, APN polynomials and related codes, J. Comb. Inf. Syst. Sci. 34 (2009) 135–159 (Special volume: Honoring the 75th birthday of Prof. D.K. Ray-Chaudhuri).
[8] C. Carlet, On almost perfect nonlinear functions, IEICE Trans. Fundamental. E91-A (2008) 3665–3678.
[9] C. Carlet, P. Charpin, V. Zinoviev, Codes, bent functions, and permutations suitable for DES-like cryptosystems, Des. Codes Cryptogr. 15 (1998) 125–156.
[10] A. Chang, P. Gaal, S.W. Golomb, G. Gong, P.V. Kumar, On a sequence conjectured to have ideal 2-level autocorrelation function, ISIT 1998, Cambridge.
[11] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): the Niho case, Inform. and Comput. 151 (1999) 57–72.
[12] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): the Welch case, IEEE Trans. Inform. Theory 45 (1999) 1271–1275.
[13] H. Dobbertin, Almost perfect nonlinear power functions on GF(2^n): a new case for n divisible by 5, in: Proc. FFA'99, Springer, Berlin, 2001, pp. 113–121.
[14] R. Gold, Maximal recursive sequences with 3-valued cross-correlation functions, IEEE Trans. Inform. Theory 14 (1968) 154–156.
[15] A. Hocquenghem, Codes correcteurs d'erreurs, Chiffres (Paris) 2 (1959) 147–156.
[16] H. Hollmann, Q. Xiang, On binary cyclic codes with few weights, in: Proc. FFA'99, Springer, Berlin, 2001, pp. 251–275.
[17] H. Hollmann, Q. Xiang, A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences, Finite Fields Appl. 7 (2001) 253–286.
[18] X. Hou, Affinity of permutations of $\mathbb{F}_{2^n}$, Discrete Appl. Math. 154 (2006) 313–325.
[19] T. Kasami, Weight distributions of Bose–Chaudhuri–Hocquenghem codes, in: R.C. Bose, T.A. Dowling (Eds.), Combinatorial Mathematics and Its Applications, University of North Carolina Press, Chapel Hill, NC, 1969, pp. 335–357.
[20] T. Kasami, The weight enumerators for several classes of subcodes of the second order binary Reed–Muller codes, Inf. Contr. 18 (1971) 369–394.
[21] G. Leander, P. Langevin, On exponents with highly divisible Fourier coefficients and conjectures of Niho and Dobbertin, in: Algebraic Geometry and Its Applications, 2008, pp. 410–418.
[22] R. Lidl, H. Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison–Wesley, Reading, MA, 1983.
[23] F. MacWilliams, N. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, The Netherlands, 1977.

[24] R. McEliece, On periodic sequence from GF(q), J. Combin. Theory Ser. A 10 (1971) 80–91.
[25] Y. Niho, Multi-valued cross-correlation functions between two maximal linear recursive sequences, PhD dissertation, Univ. of Southern California, Los Angeles, 1972.
[26] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptology – EUROCRYPT'93, in: Lecture Notes in Comput. Sci., vol. 765, Springer-Verlag, Berlin, Germany, 1994, pp. 55–64.
[27] T. Schaub, A linear complexity approach to cyclic codes, PhD dissertation, Swiss Federal Inst. Technol., Zurich, Switzerland, 1988.